The complete Windows reference — now updated for Vista!

Windows Vista™

ALL-IN-ONE DESK REFERENCE

FOR DUMMIES®

9 BOOKS IN 1

- A Vista Orientation
- Vista Boot Camp
- Securing Vista
- Customizing Vista
- Vista on the Internet
- Adding Cool Hardware
- Joining the Multimedia Mix
- Vista Video
- Setting Up a Vista Network

Woody Leonhard

Chapter 3: Windows Firewall Backward and Forward

In This Chapter

- **Discovering what Windows Firewall can — and can't — do**
- **Knowing when Windows Firewall causes problems — and how to get around them**
- **Struggling with the bare-bones outbound Windows Firewall**
- **Making Windows Firewall work the way you want**

A *firewall* is a program that sits between your computer and the Internet, protecting you from the big, mean, nasty gorillas riding around on the Information Highway. An *inbound* firewall acts like a traffic cop that, in the best of all possible worlds, only allows "good" stuff into your computer and keeps all the "bad" stuff out on the Internet where it belongs. An *outbound* firewall prevents your computer from sending bad stuff to the Internet, like when your computer gets infected with a virus or has another security problem.

Vista includes a usable (if not fancy) inbound firewall. It also includes a snarly, hard-to-configure, rudimentary outbound firewall, which has all the social graces of a junkyard dog. Unless you know the magic incantations, you'll never even see the outbound firewall — it's completely muzzled until you dig into the Vista doghouse and teach it some tricks.

Everybody needs an inbound firewall, without any doubt. Outbound firewalls are useful, but they can be very hard to understand and maintain. If you figure that you need an outbound firewall, try to use Vista's and when you (inevitably) throw your hands up in disgust, take a look at Microsoft's competitors. This chapter should help you through the minefield.

Comparing Firewalls

Vista's inbound firewall works reasonably well. It lacks many of the fancy features that you can find in competing firewalls, but for most folks, it's good enough.

On the other hand, Vista's outbound firewall doesn't hold a candle to any of the commercially available firewalls. These points explain why:

- Competitive firewalls come with a built-in passel of outbound default settings that help you get started without being tripped up by the most common outbound traffic. By contrast, Vista's outbound firewall has exactly zero built-in settings.
- You can "train" competitive firewalls by having them watch outbound traffic and then ask you to block or allow specific programs. The firewall remembers your responses and, over time, reduces its level of intrusiveness. Vista's outbound firewall, on the other hand, doesn't ask, doesn't learn, and doesn't care. If you've told Vista to block something in particular, it won't get out of your PC; if you haven't told Vista to block something, it goes through.
- Competitors attempt to put a decent interface on their firewalls: The buttons and menus may be overly cute or convoluted, but at least they try to organize the outbound settings in a reasonable fashion. As you can see in the section "Coping with Vista's Outbound Firewall" later in this chapter, Microsoft has done almost nothing to make Vista's outbound firewall easy to use. Quite the contrary. The inbound and outbound firewalls look like they came from two different planets. Which they did.

Microsoft says it disabled Vista's outbound firewall because corporate customers demanded it. That seems mighty disingenuous to me because companies running Active Directory pull all the strings on their users' desktops anyway. I think Microsoft had many reasons for making the outbound firewall so infernally hard to use, not the least of which is the fact that enforcing almost any kind of outbound firewall would've driven Microsoft's support demands through the roof.

Hardware firewalls

Most modern routers and wireless access points include significant firewalling capability. If you have a choice between connecting your computer directly to a "cable modem" (typically via a USB port) and going through a router (typically using a local-area network [LAN] connection or a wireless connection), choose the latter.

Routers and wireless access points add an extra step between your computer and the Internet. That extra jump — called Network Address Translation — combined with innate intelligence on the router's part can provide an extra layer of protection that works independently from, but in conjunction with, the firewall running on your PC.

If you find yourself spending too much time fighting Vista's firewall, consider shelling out the bucks for a top-notch firewall such as ZoneAlarm (`www.zonelabs.com`), Norton Personal Firewall (`www.symantec.com`), Trend Micro's PC-cillin Internet Security (`www.trendmicro.com`), and so on. Run a Google search on "firewall reviews" for the latest features and price comparisons.

Understanding Vista Firewall's Basic Features

All versions of Vista ship with a decent, capable — but not foolproof — stateful firewall called *Windows Firewall (WF)* (see the nearby sidebar, "What's a stateful firewall?"). WF's basic characteristics are as follows:

- **WF's inbound firewall is on by default.**
- **Unless you change something, Windows Firewall is turned on for all the connections on your PC.** So, for example, if you have a LAN network cable, a wireless networking card, and a modem on a specific PC, WF is turned on for all of them. The only way Windows Firewall gets turned off is if you deliberately turn it off, or if the network administrator on your Big Corporate Network decides to disable it by remote control, or install Windows service packs with Windows Firewall turned off (which may be a good choice, in some cases).
- **WF settings for inbound protection can be changed relatively easily.** When you make changes, they apply to all the connections on your PC.
- **On the other hand, WF settings for outbound protection make the rules of cricket look like child's play.**
- **WF kicks in before the computer is connected to the network.** Back in the not-so-good old days, a lot of PCs got infected between the time they were connected and when the firewall came up.
- **WF has an inbound "lockdown" mode.** By selecting one fairly easy-to-find Block All Incoming Connections check box (see Figure 3-1), you can lock down your computer so that it only accepts incoming data that has been explicitly requested by programs running on your computer. Any attempt by outside programs to communicate with your computer gets rebuffed. (I show you how to find this check box in the section, "Starting, Stopping, and Goosing Inbound WF," later in this chapter.)

In practice, that means you can use Internet Explorer to look at Web sites, and you can send and receive e-mail and use instant messengers, as well as using printers and folders on your local network if you have one, but most other online functions are locked out. For example, if you use the Internet to play games with other folks who are online, or if you

connect to your computer at work, locking down your PC prevents you from connecting. A lockdown even shuts down any connection to other computers or printers (or other shared devices) on the network. That's great if you're connecting in an airport and don't want other travelers to get at your Shared Documents folder. But it's a real pain in the neck in your home or office.

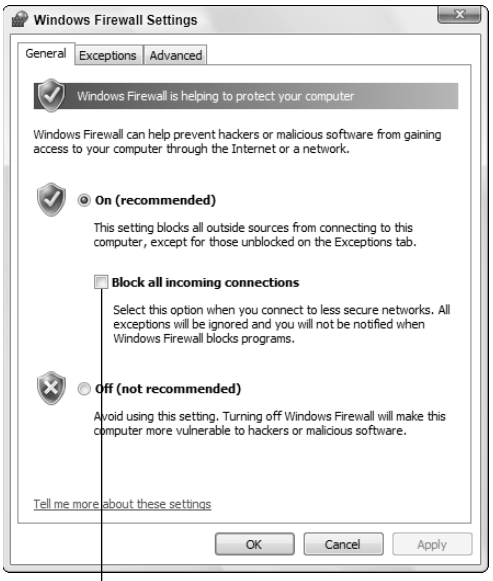
Windows Firewall Settings
General
Exceptions
Advanced
Windows Firewall is helping to protect your computer
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.
Block all incoming connections
Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.
Tell me more about these settings
OK
Cancel
Apply
Check this box and click OK to shut down all incoming traffic

Figure 3-1: The Block All Incoming Connections check box allows you to close all incoming traffic with a few clicks.

If you hear about a new worm making the rounds, you can easily lock down your computer for a day or two and then go back to normal operation when the worm stops ping-ponging over the Internet. You might need to deselect the Block All Incoming Connections check box long enough to print on a shared printer or to get at some data on your network, but you'll be essentially impenetrable whenever the Block All Incoming Connections check box is selected. If you're connecting to a strange network (say, using a wireless connection at a coffee shop or in a hotel), you can lock down while logged on and sip your latte with confidence.

What's a stateful firewall?

At the risk of oversimplifying a bit, a *stateful firewall* refers to an inbound firewall that remembers. A stateful firewall keeps track of packets of information coming out of your computer and where they're headed. When a packet arrives and tries to get in, the inbound firewall matches the originating address of the incoming packet against the log of addresses of the outgoing packets to make sure that any packet allowed through the firewall comes from an expected location.

Stateful packet filtering isn't 100 percent foolproof. And you must have some exceptions so that unexpected packets can come through for reasons discussed elsewhere in this chapter. But it's a very fast, reliable way to minimize your exposure to potentially destructive packets.

Speaking Your Firewall's Lingo

At this point, I need to inundate you with a bunch of jargon so that you can take control of Windows Firewall. Hold your nose and dive in. The concepts aren't that difficult, although the lousy terminology sounds like it was invented by a first-year advertising student. Refer to this section if you get bewildered when wading through the WF dialog boxes.

As you no doubt realize, the amount of data that can be sent from one computer to another over a network can be tiny or it can be huge. Computers communicate with each other by breaking the data into *packets* — small chunks of data with a wrapper that identifies where the data came from and where it's going.

On the Internet, packets can be sent two different ways:

- **UDP** (User Datagram Protocol) is fast and sloppy. The computer sending the packets doesn't keep track of which packets were sent, and the computer receiving the packets doesn't make any attempt to get the sender to resend packets that vanish mysteriously into the bowels of the Internet. UDP is the kind of *protocol* (transmission method) that can work with live broadcasts, where short gaps wouldn't be nearly as disruptive as long pauses, while the computers wait to resend a dropped packet.
- **TCP** (Transmission Control Protocol) is methodical and complete. The sending computer keeps track of which packets it's sent. If the receiving computer doesn't get a packet, it notifies the sending computer, which resends the packet. Almost all communication over the Internet these days goes via TCP.

Every computer on a network has an *IP address.* The IP address is a collection of four sets of numbers, each between 0 and 255. For example, 192.168.1.2 is a common IP address for computers connected to a local network; the computer that handles the Dummies.com Web site is at 208.215.179.139. I tend to think of the IP address as analogous to a telephone number.

Peeking into Your Firewall

When you add a firewall — and you should — you change the way your computer communicates with other computers on the Internet. This section explains what Windows Firewall is doing behind the scenes so that when it gets in the way, you understand how to tweak it. (You find the ins and outs of working around the firewall in the section "Making Inbound Exceptions," later in this chapter.)

When two computers communicate, they not only need each other's IP address but they also need a specific entry point called a *port* — I think of it as a telephone extension number — to talk to each other. For example, most Web sites respond to requests sent to port 80. There's nothing magical about the number 80: It's just the port number that people have agreed to use when trying to get onto a Web site's computer. If your Web browser wants to look at the Dummies.com Web site, it'll send a packet to 208.215.179.139, port 80.

Windows Firewall works by handling all these duties simultaneously:

- It keeps track of outgoing packets and allows incoming packets to go through the firewall if they can be matched with an outgoing packet. (In other words, WF works as a stateful inbound firewall.)
- If your computer is attached to a "private" network, Windows Firewall allows packets to come and go on ports 139 and 445, but only if they came from another computer on your local network and only if they're using TCP. Windows Firewall needs to open those ports for file and printer sharing. (See the next section of this chapter for the details about different network types.)
- Similarly, if you're attached to a "private" network, Windows Firewall automatically opens ports 137 and 138 for UDP, but only for packets that originate on your local network.
- If you've specifically told Windows Firewall that you want it to allow packets to come in on a specific port and the Block All Incoming Connections check box isn't selected, WF follows your orders. You might need to open a port in this way for online gaming, for example.

- Windows Firewall allows packets to come into your computer if they're sent to the Remote Assistance program (unless the Block All Incoming Connections check box is selected), providing that you created a Remote Assistance request on this PC and told Vista to open your firewall (see Book II, Chapter 5). Remote Assistance allows other users to take control of your PC, but it has its own security settings and strong password protection. Still, it's a known security hole that's enabled when you create a request.
- You can tell Windows Firewall to accept packets that are directed at specific programs. Usually, any company that makes a program designed to listen for incoming Internet traffic (Skype being a prime example, as are any instant messaging programs) adds its program to the list of designated exceptions when the program gets installed.
- Unless an inbound packet meets one of the preceding criteria, it's simply ignored. Windows Firewall swallows it without a peep. Conversely, unless you've changed something, any and all outbound traffic goes through unobstructed.

Using Public and Private Networks

Vista helps simplify things a bit by providing three different collections of security settings — actually, inbound Windows Firewall settings — each identified with a prototypical type of network:

- **Private networks** include peer-to-peer "workgroup" networks that are under your control, such as the kind you might set up following the instructions in Book IX, Chapter 2. You can let your hair down a little bit when you're on a private network. When you connect to a new network, if you tell Vista that it's a private network, Vista opens your computer so that others on the network can see it.
- **Public networks** include networks that you don't control — airports, Internet cafes, hotels — where a very real chance exists that somebody else connected to the network could go snooping, or may try to shove infected files into your Public folder. When you connect to a new network, if you tell Vista that it's a private network, Vista knows that it shouldn't make your PC visible on the network.
- **Domain networks** are Big Corporate Networks — client/server "domains." If you take your laptop to the office and plug it in to a Big Corporate Network, Vista recognizes the fact and automatically puts in place all the security that comes along for the ride. Unlike private and public networks, you don't get to tell Vista which kind of network you're using when you connect into a domain.

Establishing a network type

Each connection that you make gets associated with one of the three kinds of network: private, public, or domain. Say you have a laptop with a wireless connection. You follow the instructions in Book IX, Chapter 3 to set up a network at home called SeaBreeze. You also schlep the laptop to your friendly local Sandwich Shoppe and the Microsoft Bob Memorial Airport, and you take it to work. Vista identifies each of those four connections as public, private, or a domain network. Here's how:

- When you first make a connection to your home network, Vista asks you what kind of network SeaBreeze might be. You tell Vista that SeaBreeze is a private network in your Home (see Figure 3-2). That way, Vista allows other computers on the network to "see" your computer.
- You take your laptop to the Sandwich Shoppe and connect to the wireless network there. Vista asks whether this is a private or public network, and you respond by saying "Public."
- Similarly, you take the laptop to Patong Airport and connect to the network there. Vista asks whether this is a private or public network, and you respond by saying "Public."
- Then you take your laptop to work and connect to your company's Big Corporate Network. This time, you may not have to tell Vista anything — it knows that you're on a domain, and all the security settings that the network admin has established get pushed onto the PC. If there's any doubt, Vista asks, and you tell it you're at Work.

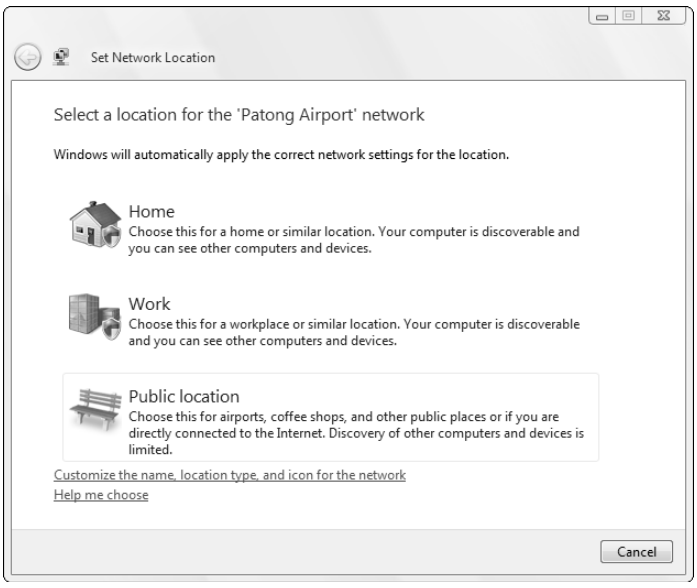
Set Network Location
Select a location for the 'Patong Airport' network
Windows will automatically apply the correct network settings for the location.
Home
Choose this for a home or similar location. Your computer is discoverable and you can see other computers and devices.
Work
Choose this for a workplace or similar location. Your computer is discoverable and you can see other computers and devices.
Public location
Choose this for airports, coffee shops, and other public places or if you are directly connected to the Internet. Discovery of other computers and devices is limited.
Customize the name, location type, and icon for the network
Help me choose
Cancel

Figure 3-2: Every time you connect to a new network, Vista asks whether it's a private (Home or Work) or Public network.

Each connection has its own Windows Firewall settings. By telling Vista whether a connection is private or public, you're actually telling Vista which bunch of Firewall settings to use initially.

When you first tell Vista that a wireless network is private, it applies the "private" firewall settings to the connection. When you tell Vista that a network is public, it applies the "public" settings. After those initial settings are in place, you can modify specific Windows Firewall settings for that connection.

Changing network types

You can change a network from public to private, or vice versa. To do so, follow these steps:

1. **Connect to the network that you want to change.**

   For example, if you want to change your laptop's connection on your home SeaBreeze network from private to public, run back home and connect to the SeaBreeze network.

2. **Choose Start⇨Control Panel. Under the Network and Internet heading, click the View Network Status and Tasks link.**

   Vista opens the Network and Sharing Center shown in Figure 3-3.

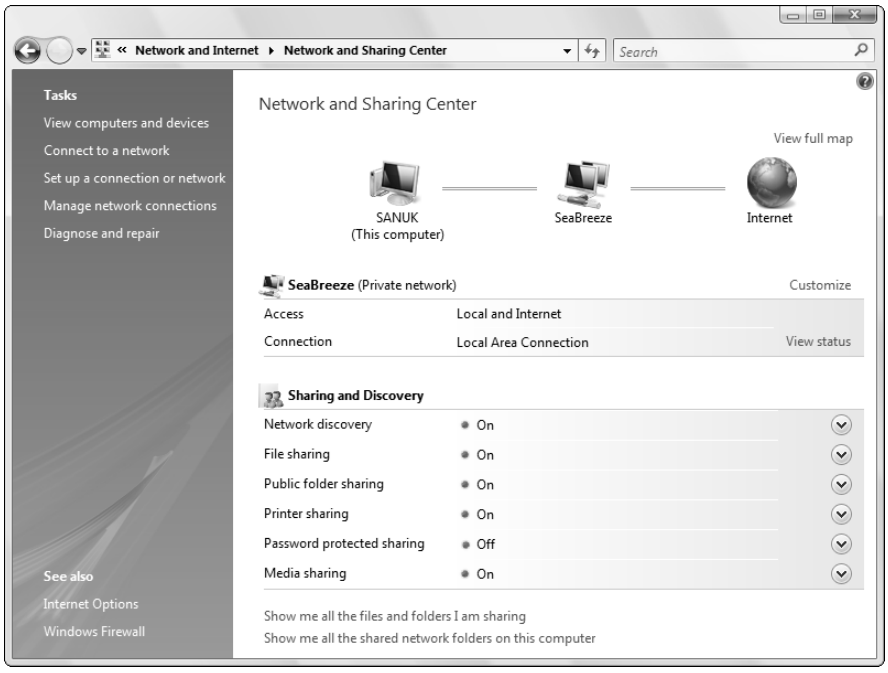

Figure 3-3: Vista's Network and Sharing Center lets you switch from private to public network settings, and vice versa.

3. **If you want to change a private network to a public network (in other words, if you want to apply the more-stringent "public" firewall settings to this connection), click the Customize link to the right of the Private Network line.**

   Vista opens the Personalize Settings for Network dialog box shown in Figure 3-4.

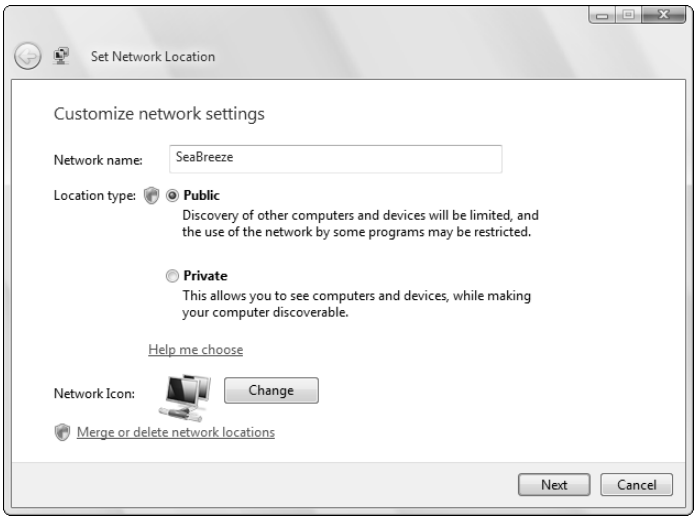
Set Network Location
Customize network settings
Network name:
SeaBreeze
Location type:
Public
Discovery of other computers and devices will be limited, and the use of the network by some programs may be restricted.
Private
This allows you to see computers and devices, while making your computer discoverable.
Help me choose
Network Icon:
Change
Merge or delete network locations
Next
Cancel

Figure 3-4: Make the switch to public here.

4. **Choose either Public or Private.**

   Remember that Public is more restricted than Private. The terminology can be a bit confusing.

5. **Click OK.**

   You may have to click through a User Access Control security dialog box, but in the end, Vista changes the category to Public.

   Vista advises you that it has successfully set your network settings. Click Close.

   You see the new Network and Sharing Center settings, as shown in Figure 3-5. Note how Network Discovery, in particular, has been turned off.

6. **Click the red *X* to exit the Network and Sharing Center.**

   The new firewall settings take effect immediately.

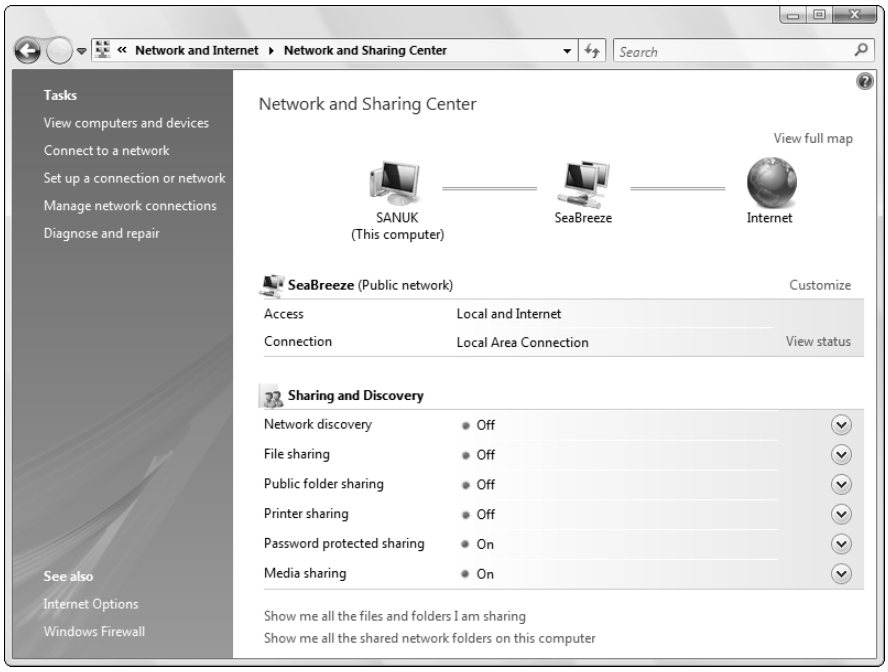

Figure 3-5: The new, more stringent, Public firewall settings, as seen through the Network and Sharing Center.

Changing individual network settings

You can modify Windows Firewall settings for each connection by using the Network and Sharing Center.

I step through my recommended settings in Book II, Chapter 1, but you can modify how much you want to share at any point.

Say, for example, that you want to allow people on your network to open files in your Public folder, providing that they can supply a user ID and password on your PC. Follow these steps to do that:

1. **Connect to the network that you want to change.**
2. **Choose Start⇨Control Panel. Under the Network and Internet heading, click the View Network Status and Tasks link.**

   Vista shows you the Network and Sharing Center (refer to Figure 3-5).
3. **To the right of the Public Folder Sharing line, click the down arrow.**

   Vista expands the Sharing and Discovery pane to show you the Public Folder options (see Figure 3-6).

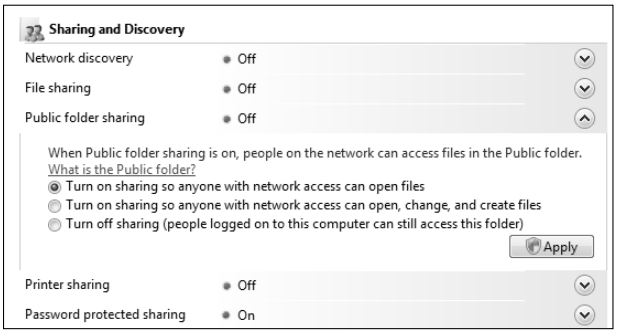
Sharing and Discovery
Network discovery
Off
File sharing
Off
Public folder sharing
Off
When Public folder sharing is on, people on the network can access files in the Public folder.
What is the Public folder?
Turn on sharing so anyone with network access can open files
Turn on sharing so anyone with network access can open, change, and create files
Turn off sharing (people logged on to this computer can still access this folder)
Apply
Printer sharing
Off
Password protected sharing
On

Figure 3-6: Allow read-only access to the Public folder with this setting.

4. **Click the Turn On Sharing so Anyone with Network Access Can Open Files option. Then click the Apply button.**

   Vista makes you click through a security dialog box and then presents you with a difficult choice (see Figure 3-7). Sharing the Public folder requires Vista to make the computer available on the network — so Network Discovery has to be turned on. But in this case, you're working with a public connection, and public connections don't do Discovery. So you have to decide whether you want to change the Public firewall settings so that *every* public connection allows Discovery and Sharing, or whether you want to change this particular connection into a private connection, which would automatically enable Discovery and Sharing on this connection? You probably want the latter.

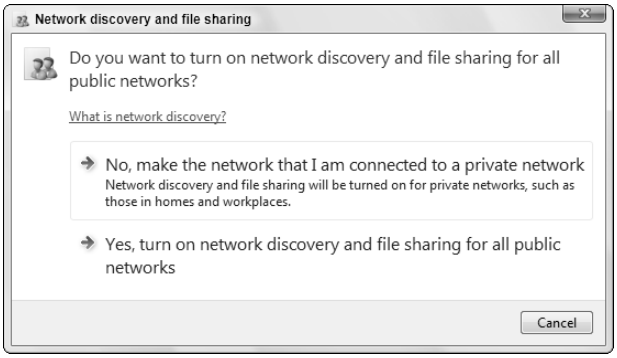
Network discovery and file sharing
Do you want to turn on network discovery and file sharing for all public networks?
What is network discovery?
No, make the network that I am connected to a private network
Network discovery and file sharing will be turned on for private networks, such as those in homes and workplaces.
Yes, turn on network discovery and file sharing for all public networks
Cancel

Figure 3-7: You should probably choose No.

5. **Click the No, Change This Network to the Network Category, Private Network and Allow Discovery and Sharing link. Then click the red *X* to exit the Network Discovery and Sharing dialog box.**

   The changes take place immediately.

Starting, Stopping, and Goosing Inbound WF

You may want to twiddle Windows Firewall on, off, or otherwise for any number of reasons. The inbound Windows Firewall is on by default, but if it gets turned off, the little Windows Security Alert icon in the System Notification area (next to the clock in the lower-right corner of your screen) should start pestering you relentlessly with "Windows Firewall is turned off" warnings.

It doesn't hurt to periodically check and be sure that your firewall is working by following these steps:

1. **Choose Start⇨Control Panel⇨Security, and under the Security Center icon, click the Check Firewall Status link.**

   You have to click through a security dialog box. Then the Windows Firewall Settings dialog box appears with the General tab showing (refer to Figure 3-1).

2. **Following the recommendations in Table 3-1, choose the setting you need.**

3. **Click OK, and then click the red *X* to exit the Security Center window.**

When you change the type of network from public to private and back, using the method in the preceding section, Vista changes entries in the Exceptions table. It does not, in effect, select the Block All Incoming Connections check box, because even with a public network, some firewalled communication usually takes place. If you want to lock down your inbound firewall and cut off *all* traffic through the firewall, you have to open the Windows Firewall Settings dialog box and select the Block All Incoming Connections check box.

Table 3-1 Windows Firewall General Settings

Setting	*Means*	*Recommendation*
On (Recommended)	Allow incoming packets that conform to the "stateful" criteria, plus any specified on the Exceptions tab.	Use this setting except when you're very concerned about locking down your machine.
Block All Incoming Connections	Only allow packets that conform to the "stateful" criteria.	Use this setting to lock down your connection. Other people on the network can't get into your machine, but you can't use printers or shared files on the "foreign" network, either.
Off (Not Recommended)	Allow all incoming packets.	If you absolutely have to get your computer talking to another computer, you may be forced to use this setting. But if you do, be very mindful of the fact that you've let your guard down completely — and turn Windows Firewall back on the moment you can.

When you install a third-party firewall, it usually asks for permission to disable the Windows Firewall. Running two firewalls at once is very tricky. I suggest you choose just one firewall and stick with it.

Making Inbound Exceptions

Firewalls can be absolutely infuriating. You may have a program that's worked for a hundred years on all sorts of computers, but the minute you install it on a Vista machine with Windows Firewall in action, it just stops working, for absolutely no apparent reason.

You can get mad at Microsoft and scream at Windows Firewall, but when you do, realize that at least part of the problem lies in the way the firewall *has* to work. (See the section "Peeking into Your Firewall," earlier in this chapter, for an explanation of what your firewall does behind the scenes.) It has to block packets that are trying to get in, unless you explicitly tell the firewall to allow them to get in. And — perhaps most infuriatingly — WF has to block those packets by simply swallowing them, not notifying the computer that sent the packet. Windows Firewall has to remain "stealthy" because if it sends back a packet that says, "Hey, I got your packet but I can't let it through," the bad guys get an acknowledgment that your computer exists, they probably can figure out which firewall you're using, and they may be able to combine these two pieces of information to give you a headache. It's far better for Windows Firewall to act like a black hole.

How do you know when you need a port?

Most first-time firewallers are overwhelmed by the idea of opening a port. Although you need to treat ports with care — an open port is a security threat, no matter how you look at it — sometimes you really need to open one. How do you know when you absolutely have to open a port? Usually, you get a phone call like this:

"Dude. My game won't hook up with your game. You got a firewall or somethin'?"

"Uh, yeah. I'm running Windows Firewall."

"Pshaw, man. You want to play Frumious Bandersnatch, you gotta open ports 418, 419, 420, an' 421."

"Does Frumious use UDP or TCP?"

"What's TeeCeePee, some kinda disease? I dunno, man. I just read in the instruction book that ya gotta have 418, 419, 420, an' 421 open. Doncha ever read the manual, dude?"

At that point, you guess that Frumious Bandersnatch uses TCP (that's the most common choice), you run through the Security Center to liberate the four ports, and you have the game working in 30 seconds flat.

You can tell WF to let packets through according to three separate criteria (see Figure 3-8):

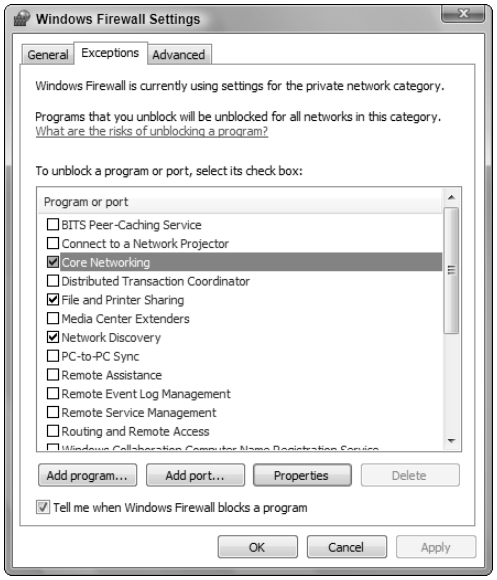

Figure 3-8: Tell Windows Firewall to allow specific kinds of packets into your PC by using the Exceptions tab.

- You'll find a list of more than a dozen predefined "services" that you can allow or disallow — for example, File and Printer Sharing, Remote Assistance, Remote Desktop, and the UPnP Framework. Many of these check boxes are selected automatically when you need them — for example, Vista selects the Remote Assistance check box when you create an Assistance request (see Book II, Chapter 5). You can manually select the corresponding check box on the Exceptions tab to allow a service.
- You can tell WF to let through any TCP or UDP packets on a specific port by clicking the Add Port button (see the "Adding a port" section, later in this chapter). You type the port number, tell WF whether you want to allow TCP or UDP, and click OK, and Windows Firewall adds the port to the exceptions list.
- You can tell WF to let through any packet that's destined to a specific program by clicking the Add Program button (see the next section in this chapter). You pick the program and tell WF whether you want to allow communication from any address on the Internet, from specific addresses on the Internet, or only from your local network. Click OK, and the firewall allows packets destined for that specific program.

File and printer sharing works by opening ports 139 and 445 for TCP over the local network and by opening ports 137 and 138 for UDP on the local network. (See the section "Speaking Your Firewall's Lingo," earlier in this chapter, for an explanation of TCP and UDP.)

If you deselect the File and Printer Sharing check box on the Exceptions tab (refer to Figure 3-8), you keep other computers on your local network from getting at your shared folders and shared hardware devices. But you also keep your computer from getting at shared folders and devices on the network.

Adding a program

Some programs need to "listen" to incoming traffic from the Internet; they wait until they're contacted and then respond. Usually, you'll know whether you have such a program because the installer tells you that you need to tell your firewall to back off. If you want to tell Windows Firewall that it should let packets through if they're destined for a specific program, follow these steps:

1. **Choose Start⇨Control Panel⇨Security, and under the Windows Firewall icon, click the Allow a Program through Windows Firewall link.**

   Click through a security box and you see the Windows Firewall Settings Exceptions tab (refer to Figure 3-8).

2. **Click the Add Program button.**

   Windows Firewall displays the Add a Program dialog box, as shown in Figure 3-9.

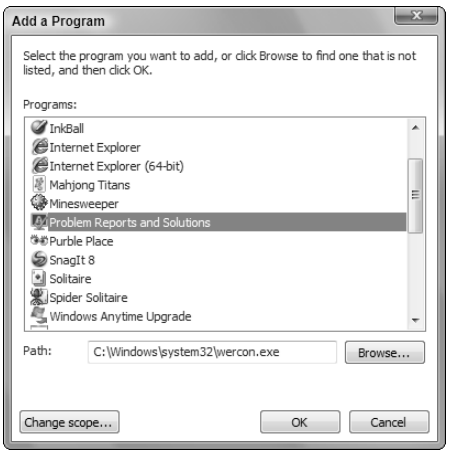

Figure 3-9: Choose the program that's the designated receiver for inbound packets.

3. **Pick the program that's designated to receive unsolicited packets from the Internet.**

   Realize that you're opening a potential, albeit small, security hole. The program you choose better be quite capable of handling packets from unknown sources.

4. **Click OK twice to go back to the Security window.**

Adding a port

Adding a port to the exceptions list is inherently less secure than adding a program. Why? Because the bad guys have a hard time guessing which programs you've left open — they have a whole lot of programs to choose from — but probing all the ports on a machine to see whether any of them let packets go through is comparatively easy.

Still, you may need to open a port to enable a specific application. When you select the check box to allow Remote Desktop, for example, you're opening port 3389. That's the security price you pay for enabling programs to talk to each other.

Follow these steps to open a port:

1. **Choose Start⇨Control Panel⇨Security, and under the Windows Firewall icon, click the Allow a Program through Windows Firewall link.**

   You get yet another security box. Click the Continue button, and you see the Windows Firewall Settings Exceptions tab (refer to Figure 3-8).

2. **Click the Add Port button.**

   Windows Firewall displays the Add a Port dialog box, as shown in Figure 3-10.

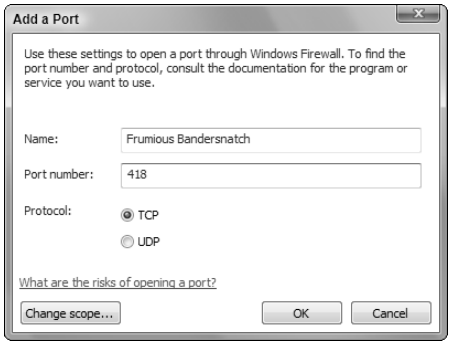
Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
Frumious Bandersnatch
Port number:
418
Protocol:
TCP
UDP
What are the risks of opening a port?
Change scope...
OK
Cancel

Figure 3-10: To open a port for any packet that tries to use it, type in a port number and specify whether it's TCP or UDP.

3. **Type the port number that you want to open. Select TCP or UDP as the protocol (if in doubt, stick with TCP), give the exception a name, and click OK.**

   See the section "Speaking Your Firewall's Lingo," earlier in this chapter, for a description of TCP and UDP.

   The Windows Firewall dialog box gets a new exception entry for the port you just entered (see Figure 3-11).

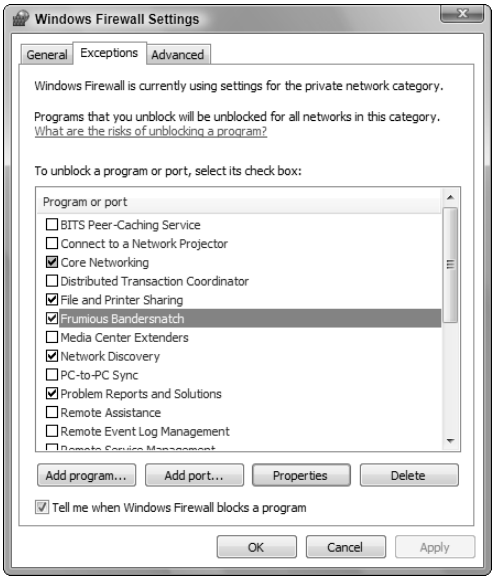

Figure 3-11: Individual ports that you add manually appear as check boxes on the Exceptions tab.

4. **Click OK to go back to the Security Center window.**

Every port that you open to the outside world is a potential location for an attack. Open ports sparingly, and when you're done, close them by deselecting the appropriate check box in the Program or Port list.

You can add only one port at a time. If you need to add ports 418, 419, 420, and 421, you have to click the Add Port button four separate times, type the pertinent information four separate times, and select four separate check boxes in the Program and Port list every time you want to block or unblock the ports. Dude.

If you have a hardware firewall (and if you use a router of almost any description, you no doubt have one going full-time), you probably need to open the same port on the hardware firewall, too. You can find an enormous amount of detailed information for poking through every imaginable router at `www.portforward.com/routers.htm`.

Coping with Vista's Outbound Firewall

Vista's outbound firewall doesn't work, look, or behave anything like the inbound firewall. Basically, it's there and it's on, but it doesn't block a thing unless you tell it to. Whereas the inbound firewall offers the different levels of settings and enables you to further tweak those settings, the outbound firewall has only two basic functions: blocking a program (or port, or something else) you select and unblocking a program you've previously blocked.

To show you how the outbound firewall works, permit me to step you through an example. Consider that (yet another) security hole has been discovered in Internet Explorer (IE) and that you want to ensure that IE isn't allowed to connect to the Internet. Perhaps you use Firefox, and you want to make sure that Vista (or Windows Media Player or Outlook or Windows Update . . .) doesn't surreptitiously crank up IE and turn it loose on the Web.

In firewall terminology, I want to block IE from making any outbound connection. Here's how to do it:

1. **Click the Start button. Immediately type** mmc **and press Enter.**

   After you click through a security dialog box, the Microsoft Management Console appears (see Figure 3-12).

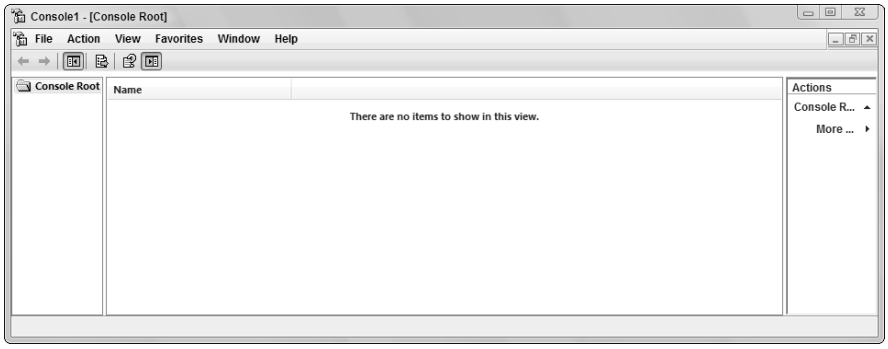

Figure 3-12: You have to use the Microsoft Management Console to make changes to Vista's outbound firewall.

2. **Choose File➪Add/Remove Snap-in. Scroll way down to the bottom of the Available Snap-ins list, choose Windows Firewall with Advanced Security, and click the Add button.**

   MMC responds with the Select Computer dialog box (see Figure 3-13).

3. **Make sure that the Local Computer option button is selected, and click the Finish button. Then click OK in the Add or Remove Snap-ins dialog box.**

   Windows Firewall with Advanced Security appears in the Microsoft Management Console dialog box.

4. **Double-click either of the two Windows Firewall with Advanced Security lines.**

   The Windows Firewall with Advanced Security (WFWAS) dialog box appears (see Figure 3-14). Note how the WFWAS snap-in maintains three separate profiles, one each for public networks, private networks, and domain networks (see the section "Establishing a network type," earlier in this chapter).

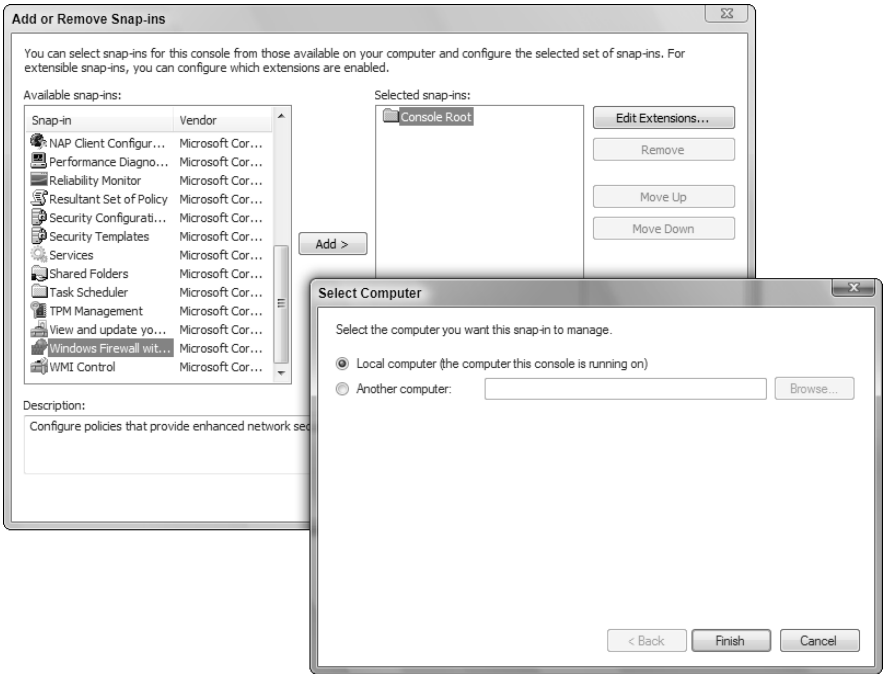

Figure 3-13: Add the Windows Firewall with Advanced Security snap-in, and enable it for the local computer.

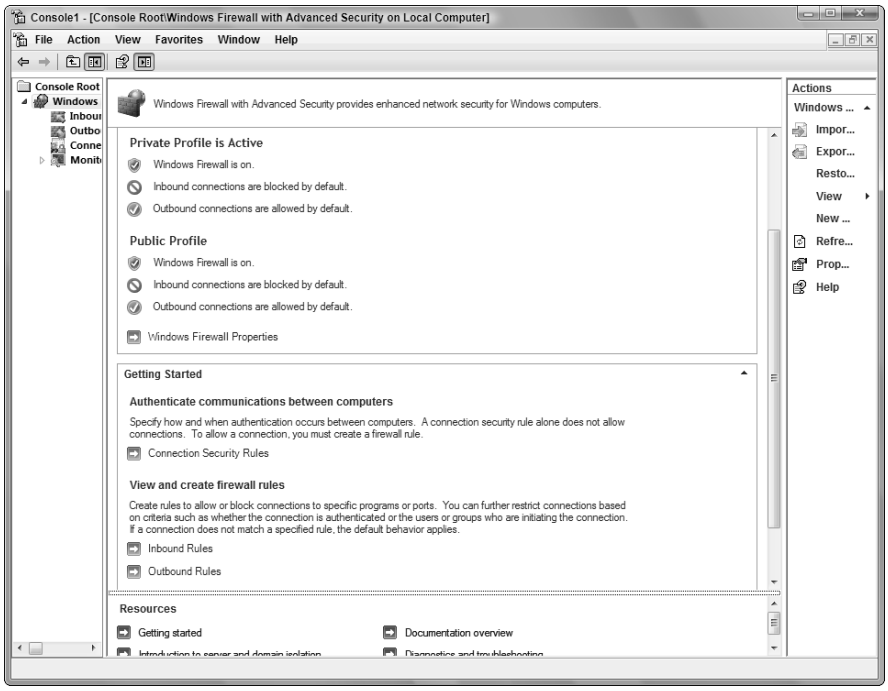
Console1 - [Console Root\Windows Firewall with Advanced Security on Local Computer]
File Action View Favorites Window Help
Console Root
Windows
Windows Firewall with Advanced Security provides enhanced network security for Windows computers.
Private Profile is Active
Windows Firewall is on.
Inbound connections are blocked by default.
Outbound connections are allowed by default.
Public Profile
Windows Firewall is on.
Inbound connections are blocked by default.
Outbound connections are allowed by default.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Specify how and when authentication occurs between computers. A connection security rule alone does not allow connections. To allow a connection, you must create a firewall rule.
Connection Security Rules
View and create firewall rules
Create rules to allow or block connections to specific programs or ports. You can further restrict connections based on criteria such as whether the connection is authenticated or the users or groups who are initiating the connection. If a connection does not match a specified rule, the default behavior applies.
Inbound Rules
Outbound Rules
Resources
Getting started
Documentation overview
Actions
Windows ...
Impor...
Expor...
Resto...
View
New ...
Refre...
Prop...
Help

Figure 3-14: The WFWAS snap-in allows you to set inbound and outbound firewall rules.

5. **In the Getting Started box, under View and Create Firewall Rules, click the Outbound Rules link.**

   WFWAS responds with a list of all the predefined rules known to Vista — and many of them exist (see Figure 3-15).

Don't mess with these rules. One mistake can lead to Dante's Seventh Ring. Trust me on this.

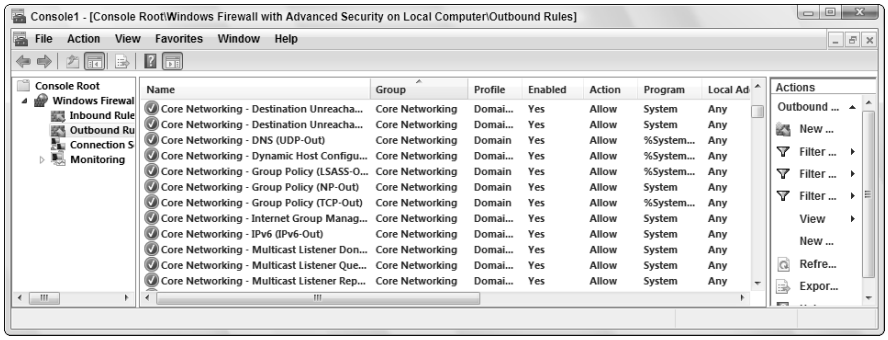
Console1 - [Console Root\Windows Firewall with Advanced Security on Local Computer\Outbound Rules]
File Action View Favorites Window Help
Console Root
Windows Firewall
Inbound Rule
Outbound Ru
Connection S
Monitoring
Name
Group
Profile
Enabled
Action
Program
Local Ad
Core Networking - Destination Unreacha... Core Networking Domai... Yes Allow System Any
Core Networking - Destination Unreacha... Core Networking Domai... Yes Allow System Any
Core Networking - DNS (UDP-Out) Core Networking Domain Yes Allow %System... Any
Core Networking - Dynamic Host Configu... Core Networking Domai... Yes Allow %System... Any
Core Networking - Group Policy (LSASS-O... Core Networking Domain Yes Allow %System... Any
Core Networking - Group Policy (NP-Out) Core Networking Domain Yes Allow System Any
Core Networking - Group Policy (TCP-Out) Core Networking Domain Yes Allow %System... Any
Core Networking - Internet Group Manag... Core Networking Domai... Yes Allow System Any
Core Networking - IPv6 (IPv6-Out) Core Networking Domai... Yes Allow System Any
Core Networking - Multicast Listener Don... Core Networking Domai... Yes Allow System Any
Core Networking - Multicast Listener Que... Core Networking Domai... Yes Allow System Any
Core Networking - Multicast Listener Rep... Core Networking Domai... Yes Allow System Any
Actions
Outbound ...
New ...
Filter ...
Filter ...
Filter ...
View
New ...
Refre...
Expor...

Figure 3-15: WFWAS lists all the available firewall rules.

6. **On the right, under Actions/Outbound, choose New.**

   WFWAS responds with the first pane of the New Outbound Rule Wizard (see Figure 3-16).

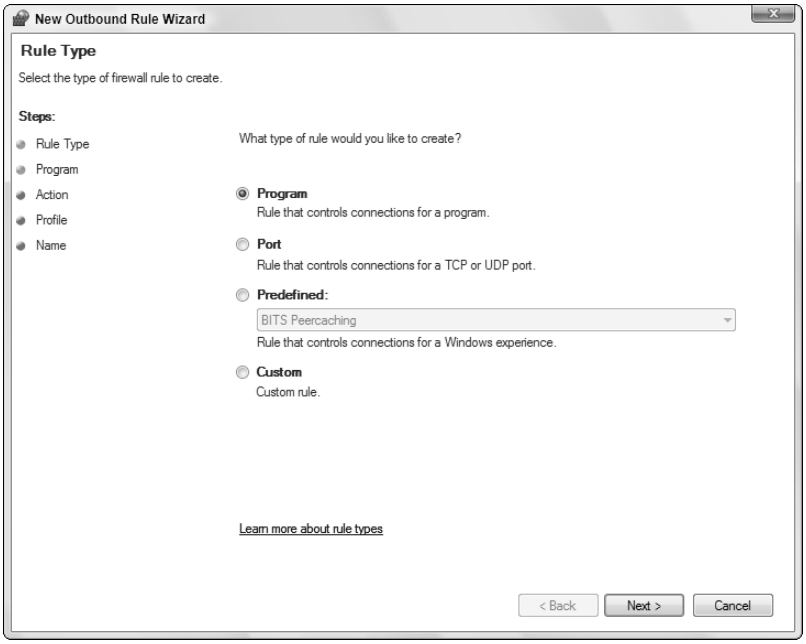

Figure 3-16: A wizard helps guide you through the creation of an outbound firewall rule.

7. **For this example, I want to block a program, Internet Explorer, so I make sure that the Program option is selected and then click Next.**

   The wizard asks whether you want the rule to apply to all programs or to a specific program.

8. **Select the This Program Patch line, and click the Browse button.**

   The wizard wants you to pick the program that's going to be blocked by this rule.

9. **In the Look In box, navigate to** `c:\Program Files\Internet Explorer`**. Then, in the Name column, click** `iexplorer.exe` **and click the Open button.**

   That tells the wizard that you want to block Internet Explorer (which is really the program `iexplore.exe`). Your wizard should look like Figure 3-17.

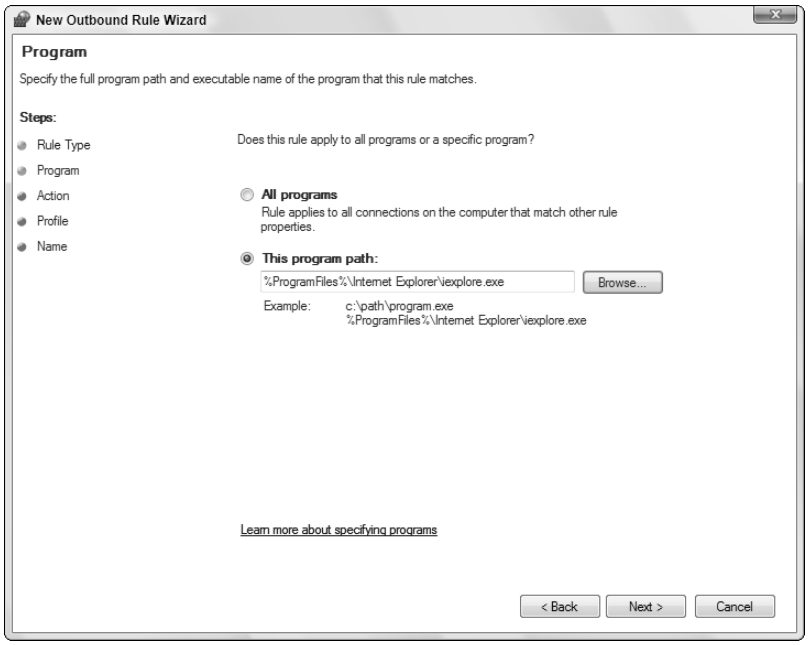

Figure 3-17: You must choose the specific program that you want to block.

10. **Click Next.**

    The wizard asks whether you want to allow the program to go through the firewall, whether you want to allow it if it obeys something called an IPsec rule, or whether you want to prohibit the program from getting out.

11. **Click the Block the Connection button, and click Next.**

    The wizard wants to know whether this rule applies to private networks, public networks, and/or domain networks (see the section "Establishing a network type," earlier in this chapter).

12. **If you want to block IE from going out over a private connection, select the appropriate check box. Similarly, to keep IE from going out over a public network connection, select that check box. Then click Next.**

    The last step of the wizard asks you for a name for the rule and gives you space to type a description.

13. **In the Name box, type something descriptive like** Block IE**. Type a description if you like, and then click Finish.**

    WFWAS puts your new rule at the top of the list (see Figure 3-18). The new block takes effect immediately.

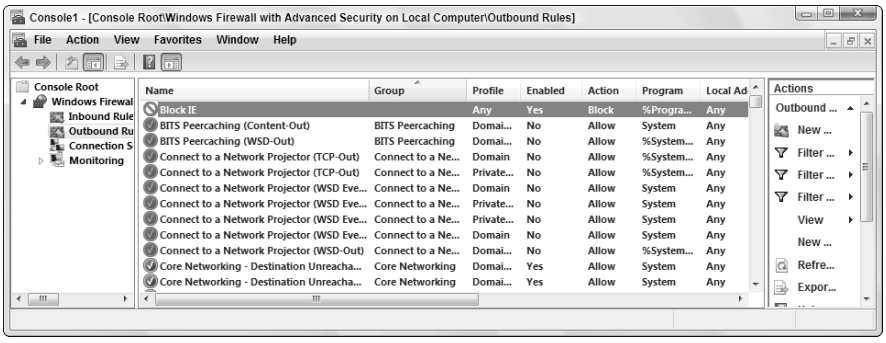
Console1 - [Console Root\Windows Firewall with Advanced Security on Local Computer\Outbound Rules]
File Action View Favorites Window Help
Console Root
Windows Firewal
Inbound Rule
Outbound Ru
Connection S
Monitoring
Name Group Profile Enabled Action Program Local Ad
Block IE Any Yes Block %Progra... Any
BITS Peercaching (Content-Out) BITS Peercaching Domai... No Allow System Any
BITS Peercaching (WSD-Out) BITS Peercaching Domai... No Allow %System... Any
Connect to a Network Projector (TCP-Out) Connect to a Ne... Domain No Allow %System... Any
Connect to a Network Projector (TCP-Out) Connect to a Ne... Private... No Allow %System... Any
Connect to a Network Projector (WSD Eve... Connect to a Ne... Domain No Allow System Any
Connect to a Network Projector (WSD Eve... Connect to a Ne... Private... No Allow System Any
Connect to a Network Projector (WSD Eve... Connect to a Ne... Private... No Allow System Any
Connect to a Network Projector (WSD Eve... Connect to a Ne... Domain No Allow System Any
Connect to a Network Projector (WSD-Out) Connect to a Ne... Domai... No Allow %System... Any
Core Networking - Destination Unreacha... Core Networking Domai... Yes Allow System Any
Core Networking - Destination Unreacha... Core Networking Domai... Yes Allow System Any
Actions
Outbound ...
New ...
Filter ...
Filter ...
Filter ...
View
New ...
Refre...
Expor...

Figure 3-18: The rule blocking IE appears at the top of the WFWAS list.

14. **Go ahead and try it. Try to get Internet Explorer to work. I dare ya.**

    No way. IE gives you the notice "Internet Explorer cannot display the webpage." Heh heh heh.

15. **To get rid of the rule, right-click it and choose Delete. When WFWAS asks whether you are sure that you want to delete the rule, click Yes.**

    Try Internet Explorer again, and it works like a champ.

Imagine setting up rules like that, manually, for every program that you want to block from going out on the Internet. Now you know why I say that Vista's outbound firewall is an ornery, snarly piece of software.

Individual program blocking's only part of the story, of course. If you set the outbound firewall to trap everything headed out of your machine, you'd probably spend most of your waking hours for the next ten years writing exceptions similar to this one, to allow "good" programs to get out.

Decent commercial firewalls have a long list of "good" programs. If they detect the presence of a "good" program, they poke a hole through the firewall for you. You're left with a brief (but intense) training period, where you have to approve each new, unidentified program that's trying to get out — and where you have to track down every outbound request that looks suspicious. It isn't easy, but it is tractable.

Vista's firewall doesn't work that way. You get to do all of the heavy lifting. And you get to perform that work with a user interface — the Microsoft Management Console — that has been known to bring accomplished system administrators to tears.

If you have a specific program that you want to block, Windows Firewall can do the job. But for anything other than blocking the outbound actions of a small number of targeted programs, Vista's outbound firewall rates as a marketing point ("Yes, Vista has an outbound firewall!") and little more.

Chapter 1: Preparing a Media Center PC

In This Chapter

- **Figuring out where all those %$#@! wires go**
- **Connecting your TV**
- **Surrounded by sounds**

By the time you finish putting together your first Windows Media Center (MC) system, you may swear off assembling PCs ever again. If you can get it all in one box, you have it made. But the minute you start mixing and matching, adding home theater sound here, slapping around a set-top TV box there, and wedging that 120-inch LCD screen somewhere in the middle, you're going to find out a lot more than you ever wanted to know about Dolby 7.1, IR blasters, and DVI connectors. In fact, one of the very best reasons for buying an MC component system from a local store is that you can hire the company that sold you the unit to put it together for you.

Not long ago, a friend of mine told me that he was getting out of the computer business because it's just gotten too complicated. He made that announcement — you guessed it — immediately after assembling a Windows Media Center PC. Of course, he built it from scratch. Definitely a fool's task.

Media Center PCs combine all the frustrations of assembling a complicated PC with the joys of figuring out how to attach your satellite box, where to hook up the speakers, which stack of books to stick under the TV, how to keep all the wires from pulling each other out, and what to do with the subwoofer. The only saving grace? You don't have to worry about a VCR. Probably.

Do You Need Media Center?

If you have to ask the question, you don't. Media Center ships in Windows Vista Home Premium and Ultimate editions. If you have Home Basic or either of the Business editions, you might wonder whether it's worth the bucks to upgrade.

Media Center draws people in with its incredible interface; its power; its seductive, immersive multimedia capabilities; its position as the physical and logistical center of all your audio and visual equipment — and the ability to control all that and more with a remote from across the room. With the Xbox Media Center extender, your game machine can tap into the full Vista Media Center as well. And do it, uh, well.

Here's what Media Center offers that most people want:

- The ability to record TV shows with instant-action replay (yes, it keeps recording the halftime show while you watch Justin Timberlake again), easy recording setup via a program guide, and a tiny TV mini-screen that appears just about everywhere you might want it. Best of all, you can copy the recorded TV shows (at least, the ones that aren't protected, like HBO broadcasts) to DVD.
- The full spectrum of Windows Media Player capabilities (they're extensive — see Book VII, Chapter 1), with a gorgeous user interface, all wide-screen friendly, all accessible via remote.
- A window into Vista's Photo Gallery (see Book VII, Chapter 4): one central location for all your photo stuff — transferring pics and videos from a camera, playing videos, ripping and burning CDs and DVDs, leafing through photos, running slide shows, and making prints.
- Internet Explorer, sorta, on a big screen, controlled by remote.
- All the bells and whistles you would expect from a souped-up PC that's wired for sound. And video. If you have good audio or video equipment, you'll want to control it through Media Center.

That said, Media Center isn't for everybody. In particular, it has these drawbacks:

- **Bugs:** Media Center has gone through more than its fair share of bugs over the years. With deep hooks into Vista, Windows Media Player, Photo Gallery, Internet Explorer, and a half-dozen lesser luminaries in the Windows pantheon, Media Center falls prey to bugs in many of the major Windows applications — and it adds another layer, all by itself. If swatting bugs and rebooting your computer gives you the willies, give Media Center a pass.
- **Limitations:** Limitations are legion. As of this writing, you can drive a TV screen from your Media Center system, but you can't control another PC. An hour of recorded TV takes up more than a DVD's-worth of space, unless you use the "Fair" quality setting.

Of course, the biggest limitations center around Digital Rights Management, and they aren't all exclusive to Media Center. If you record your favorite TV show on your Media Center system (in "Fair" quality, of course), can you burn it to DVD and then watch the DVD on a neighbor's DVD player? On another PC? The answers aren't cut-and-dried. If you rip a CD that you bought on your Media Center computer, can you play the tracks on your iPod? Can you play them on the computer in the bedroom? Can your son take them to school on his portable? Sure, you can use Media Center (with its direct link to Media Player) to buy music from URGE and other companies that give Microsoft a cut, but if you buy a song from iTunes, can you play it on your Media Center PC? Tough questions. If they concern you, ask people who own and use Media Center (at, for example, `http://channels.lockergnome.com/media`) before you buy.

Windows Media Center remains the 800-pound gorilla of the genre: When Comedy Central thinks online, it thinks Media Center, with content that's specifically WMC friendly, and adapted to Media Center through-and-through (see Figure 1-1.) The same with NBC and ESPN. Time Warner may be another story, but . . . if you want to stay near the bleeding edge of computerized home entertainment content, Media Center's the product of choice.

Figure 1-1: Comedy Central thinks Media Center, appearing front and center on the Media Center Showcase.

Organizing the Normandy Invasion

So you have eight big boxes sitting on your living room (or dorm room or office) floor, and the first debilitating pangs of buyer's remorse have set in.

That's normal. Not to worry. The following sections offer a handful of tips that can help you through the assembly process. Go ahead and benefit from others' experience.

Gathering the tools for an easier setup

The folks at the computer store sold you everything that you need. But I can *guarantee* they forgot a couple of items that you will surely want. Before you assemble the beast, you need to run out and pick up what they forgot.

In particular, you need the following items:

- **A UPS (uninterruptible power supply):** If the sales droid let you walk out of the shop without a UPS, he should be lashed. No, a surge protector isn't good enough. You need a UPS big enough to handle your computer and any other sensitive hardware that's hanging around: TV, network hub, DSL or cable modem, scanner, external drives, or USB hubs — the whole nine yards.

  No, you don't need to plug your printer into a UPS — and you should *never* plug a laser printer into a UPS. Laser printers draw a tremendous amount of power; a laser printer will probably blow out your UPS when it starts, and even if your UPS doesn't end up a heap of smoldering goo, if the power goes out, the UPS will die in seconds from the laser printer's power drain.

- **Lots of power strips:** The ones that plug into the UPS don't need surge protection, but any that plug straight into the wall should have surge protectors.

  Anything with a "brick" that converts AC current to DC (which you commonly find with laptop computers, telephones, modems, and so on) doesn't require a surge protector. But any brick located at the end of a power cord will invariably take up two (or even three) slots on a power strip.

- **A roll of masking tape and a fine-point permanent-ink marker:** You should mark the end of every cable as you connect it: Wrap a piece of tape around the wire and write down where it's going. That way, when you look at a power strip with five plugs in it, you can tell which one goes to your PC and which one goes to your TV. You'll also be able to tell your left-front speaker from the right-side and center-rear without pulling the speaker cable out from under the rug.

If you save a snapshot of the final array of cables — even if you only use your Webcam — you'll have a good record of which cable went where, in case your three-year-old nephew decides to pull a few cables off the back of the TV.

- **Those little plastic gizmos that bundle cables together:** They're cheap, and they'll keep you from going nuts. By the time you're done, the back of your PC is going to look like a wiring bundle down the fuselage of a 747.
- **Video cables that are long enough to go where they need to go:** Before you assemble the beast, block out precisely where the PC will go, where the monitor will go, and where the TV (if you have one) will go. Then figure out how long the video cables must be. Then dig into the box and see whether the cables you have are long enough. I bet they aren't, particularly if you're connecting a TV. When you go out shopping, make sure that you get the right kind of cables.

You can try to figure out whether you need a composite RCA cable, an S-VHS cable, a DVI cable, or a reversible 3-plug mini-DIN with imploded wombat RJ-945 cable, but why sweat the hard stuff? If you have any doubt about what kind of cable you need, haul out your digital camera and take close-up shots of the connectors on the back of your computer and on the back of your TV. Then schlep the camera to the shop, and ask the salesperson to figure it out. Hey, that's what he's paid to do.

- **Speaker cables that are long enough to go . . . well, you get the idea:** I swear, the speaker cables that ship with Media Center PCs are never long enough. Make sure that you get the right kind of connectors on the ends. No, I never pay extra for ultra-fancy cables, but you might want to.
- **Remote hardware:** Some Media Center PC systems don't have keyboards or mice. I think that's a huge mistake. At least until Microsoft brings more functions into the Media Center umbrella, occasional trips out to Windows itself are inevitable — and for those, you're going to want a keyboard and mouse. If your Media Center PC sits in a cramped dorm room, running for the keyboard is no big deal, but if you have to get up off the couch and find a chair to put in front of the computer, it's a pain in the neck.
- **A nice bottle of wine:** Need I explain what this is for? Beer does in a pinch.

Working with Media Center's shortcomings

Every Media Center PC goes together a bit differently, and the instructions (for most systems, anyway) cover the details pretty well. In my School of Hard Knocks surveys, several readers have offered a few key assembly tips that overcome several of Media Center's shortcomings:

- **Media Center (as of this writing) doesn't allow you to watch one TV show while recording another one.** If you ever find yourself in a position where it'd be worthwhile to watch one show while recording another, consider using an old trick: Split the input line. Run one set of cables from the cable box to the Media Center PC. But run a second set of cables from the cable box straight to the TV and attach the cables to the Video 1 or AUX input. To watch live TV, just switch the TV over to Video 1, ignoring the Media Center PC.

- **Media Center doesn't work with VCRs.** You can think of it as benign neglect. I think of it as a failure to accept ubiquitous legacy hardware. Potato/potahtoe, you know. At any rate, you can still hook up your VCR, and Media Center can be, uh, coaxed into recording directly from your old videotapes. The process is not for the timid, but it's covered in depth in *Windows XP Media Center Edition 2004 PC For Dummies*, by Danny Briere and Pat Hurley (published by Wiley), where you might find some good tips that pertain to Windows Vista as well. Good book, that.
- **Don't hesitate to use your current sound system.** If you have a better sound system than the one that ships with your Media Center PC, your old sound system accepts digital optical cable input, and your Media Center PC has a digital optical output on the sound card or the motherboard, go right ahead and hook it up.

Also remember that you're under no obligation to attach everything. If you don't want to run your television through the Media Center PC, you don't have to.

Getting Windows in Gear

The first time you start your new Media Center computer, almost anything could happen. Why? Each manufacturer seems to have a different way of introducing you to the experience.

Making your video card acquiesce

If your Media Center PC came with its own TV set, if you're running videos on your computer monitor, or if you already have things set up so that video stuff shows up on your TV and computer stuff shows up on your monitor, breathe a sigh of relief and move on to the next section in this chapter to verify that your sound card is working right.

But if you want to connect both a TV and a computer monitor to your PC, and haven't yet figured out how to get movies to play on the TV instead of in a window on your PC's monitor, you have a bit of work to do.

Here's how things work with an NVIDIA video card. Your graphics card may be a little different. Each video card manufacturer does things differently, but the problems and their solutions are roughly the same.

Here's the core of the problem: Your video card probably has three connectors on the back. In the normal course of events, only two of the connectors work at the same time: One handles computer stuff (which appears on your computer monitor) and the other handles video stuff (which appears on your TV). You have to tell your video card which connector has the computer monitor and which has the TV. Here's how:

1. **Connect the cables.**

   Each board is a little different, and each TV is a little different. But you need to attach your computer monitor to the video card (probably with a VGA cable, or a DVI cable if you have a newer monitor) and your TV to the video card (probably with an SVHS cable or the three-cable red/green/blue "made for DVD" connectors, but possibly with a DVI cable or some other combination).

2. **Identify your video card.**

   Video companies change drivers like Paris Hilton changes traveling companions. To make things worse, Microsoft Update may not even advise you when a new video driver becomes available. To make sure that you get the latest, click the Start button, right-click Computer, and choose Properties➪Device Manager from the context menu that appears. Click the Continue button to get through the User Account Control dialog box, and then double-click Display Adapters. You should see your display adapter listed, as shown in Figure 1-2.

3. **Update your video driver.**

   To do so, double-click your display adapter, click Continue to get through the User Access Control box, click the Driver tab, and then click the Update Driver button. When Vista asks, click the Search Automatically for Updated Software link. Vista goes out to the Microsoft Web site to see whether a new video driver is available. If it is, the driver may be updated automatically (and your screen may go black for a moment — don't panic). You may have to follow some other instructions to install the new driver. Click OK to exit the Driver dialog box, and then click the red *X* to exit Device Manager.

4. **Reboot the computer.**

   Make sure that the TV is turned on and tuned to the correct input so that it can receive signals from your computer.

   Rebooting probably isn't necessary in all cases, technically, but it's a good idea.

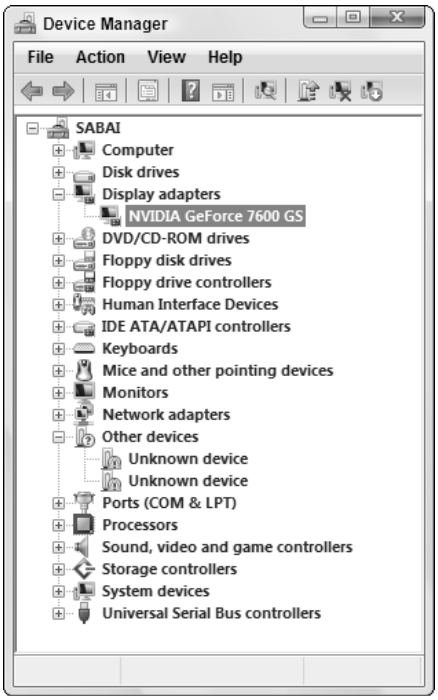

Figure 1-2: Device Manager tells you which video card you're using.

5. **Bring up the video driver manufacturer's control panel.**

   Unfortunately, this can be a bit tricky; you may need to consult your video card (or PC) user's manual to see how to do this. To bring up the NVIDIA control panel, choose Start⇨Control Panel, click the Classic View link, and then double-click the NVIDIA Control Panel icon. Ultimately, you see a dialog box like the one shown in Figure 1-3.

6. **Click through to the dialog box that lets you choose which connectors to use.**

   The NVIDIA Control Panel requires you to click the Display icon and then another button to set preferences, finally arriving at the dialog box shown in Figure 1-4.

7. **Set your display adapter to use the two displays independently.**

   NVIDIA calls it "Dualview," but regardless of the terminology, the idea is that you have two, independent pictures on the two monitors. One may be an "extended desktop" for the other. But you have to use the two separately so that computer stuff shows up on the monitor and video stuff shows up on the TV.

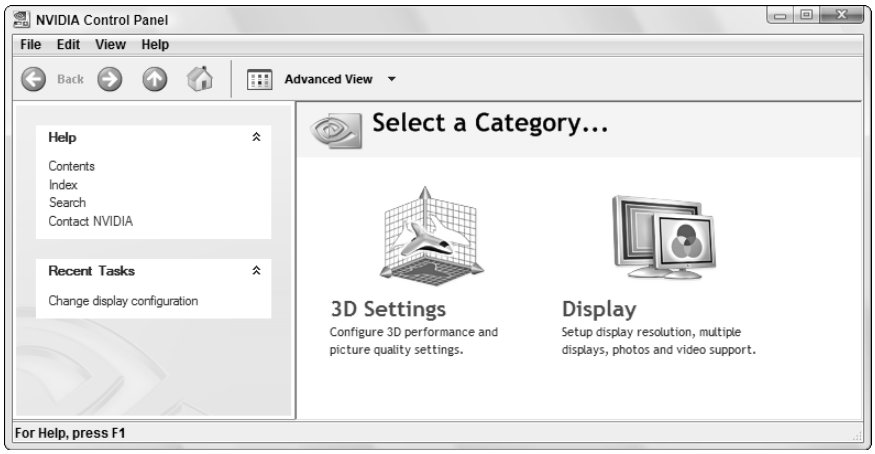

Figure 1-3: The NVIDIA Control Panel.

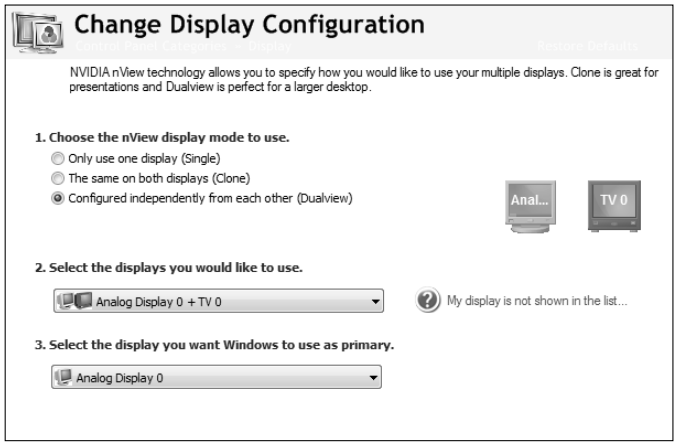
Change Display Configuration
NVIDIA nView technology allows you to specify how you would like to use your multiple displays. Clone is great for presentations and Dualview is perfect for a larger desktop.
1. Choose the nView display mode to use.
Only use one display (Single)
The same on both displays (Clone)
Configured independently from each other (Dualview)
Anal...
TV 0
2. Select the displays you would like to use.
Analog Display 0 + TV 0
My display is not shown in the list...
3. Select the display you want Windows to use as primary.
Analog Display 0

Figure 1-4: Tell the display adapter which connectors to use.

8. **Click OK as many times as necessary to exit the Control Panel, and then reboot your computer.**

   Again, a reboot may not be absolutely necessary, but it wouldn't hurt.

Congratulations! Your Media Center PC can now see double.

Setting sound straight

Modern audio cards produce phenomenal sound. If you have a home theater (that is, audio) system to provide the oomph, Media Center can rock your

house off its foundation. Kinda adds a new dimension to the old adage "if the house is a-rockin'" . . .

Setting up a sound system usually entails matching up the audio card's outputs (pink, blue, lime green, black, orange, tutti-frutti) to the audio amp's inputs, and then snaking a lot of wires over, under, around, and through the room. When you're done, the $64,000 question arises: Did you get the speakers hooked up right? Easy to ask. Not so easy to answer.

Every sound card works differently, but most of them can help you verify that the right plug on the back of the card is connected to the left, er, right speaker. For example, the Realtek AC'97 Audio chip (which ships on many AMD motherboards) can be tested in this way:

1. **Choose Start➪Control Panel➪Hardware and Sound➪Sound.**

   Vista opens the Sound dialog box, like the one shown in Figure 1-5.

Figure 1-5: The Sound dialog box for the Realtek AC'97 Audio chip.

2. **Click the Speakers icon, and then click the Configure button.**

   The Speaker Setup wizard appears, as shown in Figure 1-6.

3. **Choose the kind of speaker setup you have.**

   The diagram changes based on your selection. For example, 5.1 Surround uses two front speakers, two back speakers, a center speaker, and a subwoofer. If you click 5.1 Surround, the diagram on the right shows five speakers plus a subwoofer.

4. **Click the Test button to test each speaker, in turn, or click an individual speaker to make sure that it's properly identified.**

   If the wrong speaker sounds off, you probably messed up one of the color-coded connections on the back of the audio card. Rearrange the cables and try, try again.

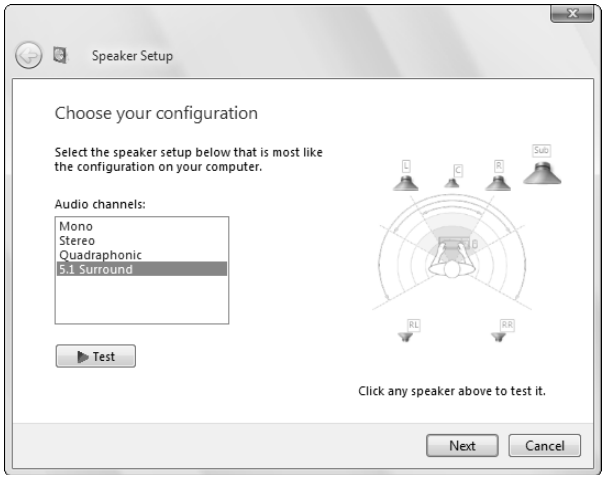

Figure 1-6: Test your speakers to make sure that they're hooked up properly.

5. **When you're done with a sound check, you can further customize the speaker layout by clicking Next, and work with the speaker configuration dialog shown in Figure 1-7.**

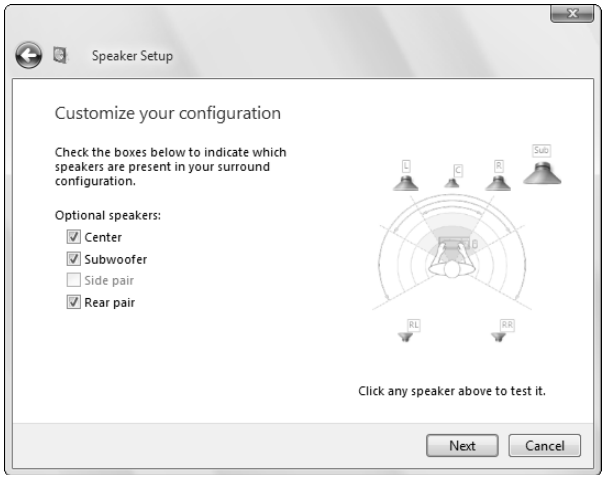

Figure 1-7: Vista gives you a great deal of control over your sound.

Or, you can click Cancel to exit the Sound dialog box; then click the red *X* to exit the Control Panel.

You're now ready to faithfully reproduce the sound of point-one hand clapping, in full 5.1 (or 7.1 or, heck, 149.1) surround sound.